**Remarks of Patrick Dwyer**

**Michigan Hearing Testimony**

**January 20, 2016**

Good morning/afternoon, my name is Patrick Dwyer, and I am Vice President U.S. State Government Affairs, at MasterCard. I would like to thank the Chairman and Committee for the opportunity to speak today on the move to EMV Chip Card Technology in the United States.

The MasterCard network connects financial institutions, merchants and cardholders ensuring payments are consistent, reliable, efficient and secure. It is a technology infrastructure connecting over 30 million merchants, 20,000 financial institutions and two billion cardholders worldwide. It is worth bearing in mind that MasterCard does not issue payment cards of any type, nor does it contract with merchants to accept those cards. Increasingly we are playing a leading role in the development of new technologies intended to secure the global payments system against criminal attack.

Chip card technology (known as EMV) uses a small computer processor embedded in the card, to authenticate a card transaction rather than the traditional magnetic strip. It enables more sophisticated authentication than previously and makes the cards impossible to counterfeit. I will take you through a presentation on exactly how this works shortly. First, however, I want to spend some time giving you background and context on how we got where we are, and why MasterCard has been working alongside all participants in the payment ecosystem to better secure consumer payment data.

As you are all aware, payment card fraud in the United States has been rising for some time. Several major data breaches have drawn considerable attention from policymakers and have raised questions about data security and the innovative technologies that might ensure safer payments.

MasterCard along with Europay and Visa (hence the name EMV) created the EMV standard over 15 years ago. EMV is managed today by EMVCo, an independent standards organization that continues to refine a globally consistent approach to payments security.

Since the introduction of EMV, we have driven the implementation of standards in markets across the globe, allowing for higher levels of security and global interoperability in payments. In markets that have implemented EMV, counterfeit fraud has decreased dramatically.

In 2012, MasterCard took an important proactive step by announcing our roadmap for U.S. migration to the EMV standard. We understood that the United States is the largest and most complex retail payments market in the world and that therefore it would take significant planning, investment and cooperation from all relevant parties for a successful migration.

While the roadmap has many elements aimed at securing all card payment channels, the most significant milestone was the liability shift on October 1, 2015, which holds the party in a transaction (card issuer or merchant) that uses the least secure technology, liable for fraud. Subsequent liability shifts for ATM transactions will take place in October this year and for gas station furl pumps in October 2017.

Incidentally, the use of EMV cards in gas stations will eliminate the scourge of the "skimmer" devices which criminals install inside gas pumps to steal cardholder data and which the Michigan Department of Agriculture and Rural Development has reported finding across the state in the past few weeks.

The move to chip cards is, naturally, headline news, as millions of Americans receive new chip-enabled cards and retailers implement new procedures at checkout. It is vitally important, however, to see this in context. Technological advances in payments security have been significant since the first EMV cards were introduced in Europe, 15 years ago. The US is introducing these cards in a much different environment, and this, we believe, gives us the opportunity to make the electronic payments system more secure than ever.

It is also important to understand that the introduction of EMV in the U.S. does not change MasterCard's Zero Liability program. As a MasterCard cardholder, zero liability applies to your

purchases made in the store, over the telephone, online, or via a mobile device and ATM transactions. MasterCard cardholders will not be held responsible for unauthorized transactions.

Today, the majority of fraud in U.S. payments comes from the electronic theft of cardholder data. This must be tackled holistically and the move to chip cards is a single, albeit vital element of a much larger move to what the payments industry calls the "secure-all-channels" strategy.

This strategy encompasses standard setting, through the Payment Card Industry Security Council; migration to new technologies (of which EMV is one); and a host of other initiatives intended to ensure that however an electronic payment is made – in person in a store, over the phone, or on the Internet, cardholder data is as secure as possible.

Chip cards have a vital role to play in this, reducing counterfeit fraud at the point-of-sale, but the payments industry is also refining complementary technologies to address the card-not-present space and other areas targeted by criminals. Much of the focus here is on devaluing cardholder data, so should a criminal get hold of it, it is worthless to them.

Point-to-Point Encryption (known as "P2PE") protects data in transit at the point-of-sale, often at the card reader, before it is sent onto a merchant's system. This means that if hackers were to intercept it through the use of increasingly common point-of-sale Malware, the data yield would be worthless. It is interesting to note that the majority of the high-profile data breaches of the last few years involved criminal use of point-of-sale Malware

Similarly, MasterCard has led the industry toward tokenization, an advanced technology that addresses card-not-present fraud by devaluing data stored in a merchant's system, replacing account numbers with one-time-use payment tokens that are useless if compromised. In October 2013, MasterCard, along with Visa and American Express, introduced a proposed framework for a tokenization standard.

Tokenization is important because it delivers more security to contactless and InApp payments by including a dynamic component with each transaction that cannot be duplicated. It is this technology that secures Apple Pay, Samsung Pay and other new smartphone based payment platforms.

These technologies are crucial in protecting us against data breaches. Nevertheless, the overwhelming majority of payment fraud in the US is counterfeit fraud and that is what EMV chip technology is intended to stop. EMV has proved very effective in reducing counterfeit fraud in every other market into which it has been introduced. For example, in the United Kingdom, which underwent a liability shift in 2006, domestic fraud reached its lowest levels ever in 2011. Similar results were seen in Canada and Australia in 2008 and 2012, respectively.

While its primary purpose is reducing counterfeit fraud by requiring an interaction between the chip card and an EMV terminal which criminals could not replicate, EMV technology provides an additional opportunity to reduce "lost or stolen" and "card-not-received" fraud, through a secondary form of authentication.

When EMV was first introduced, 15 years ago, this authentication was limited to signature or Personal Identification Numbers (PIN). As technology has developed, however, even more secure forms of authentication have been introduced like biometrics, which read fingerprints, vein patterns, heartbeats, or voice patterns. These new technologies seem likely to provide better authentication in a way that inextricably ties a chip card to a cardholder.

We believe it is in the best interests of a secure payments system if we allow authentication methods to evolve as technology changes. This is why MasterCard does not mandate a specific or a single authentication method. To mandate what is, in effect, a *static* authentication method, would, we believe, run the risk of stifling innovation in the area of payments security and act as a disincentive for adoption of more *dynamic* authentication methods.

Instead of mandating PIN authentication, MasterCard has incorporated the relative security of PIN in its liability shift rules. Much like the counterfeit liability shift for chip-enablement, MasterCard's liability shift hierarchy structure benefits the party that uses the most secure authentication method, whether that is PIN now or a more secure method in the future.

As such, if an issuer does not authenticate a given transaction with PIN, but the terminal is PIN-enabled, the merchant is protected from any resulting lost or stolen fraud, as liability rests with the issuer, not with the merchant. This provides an incentive for PIN capability to be used more

broadly—without mandating it—just like the overall liability shift incentivizes the market to move to chip but without mandating it.

We believe that innovation, and ultimately, security is best served by allowing issuers and merchants to choose how to deploy EMV chip technology based upon their business model and customer base. This flexible approach incentivizes participants in the payment ecosystem to deploy the safest and most secure tools in their business and protect consumers from fraudsters.

So, that's some background on the need for EMV migration, its place in the wider secure-all-channels strategy and our thoughts on secondary authentication. I now want us to turn our attention to our presentation which I hope will reinforce some of these points, while explaining how EMV works and what we expect it to achieve.